A CHARACTERIZATION OF A PRIME p FROM THE BINOMIAL COEFFICIENT $\binom{n}{p}$ WITH $n > p+1$ A NATURAL NUMBER

ALEXANDRE LAUGIER and MANJIL P. SAIKIA[1]

Abstract. We complete the proof of a theorem that was inspired by an Indian Olympiad problem, which gives an interesting characterization of a prime number p with respect to the binomial coefficients $\binom{n}{p}$, where $n > p+1$ is a natural number. We give an alternate proof of the theorem and mention a few consequences that can be derived from it. In the way we give a possibly new proof of Lucas' Theorem.

Key Words: prime moduli, binomial coefficients, Lucas' theorem, order modulo p, floor function.

2010 Mathematical Reviews Classification Numbers: 11A07, 11A41, 11A51, 11B50, 11B65, 11B75.

1. Introduction and Motivation

Problem 1.1. *7 divides* $\binom{n}{7} - \lfloor \frac{n}{7} \rfloor$, $\forall n \in \mathbb{N}$.

The above appeared as a problem in the Regional Mathematical Olympiad, India in 2003. Later in 2007, a similar type of problem was set in the undergraduate admission test of Chennai Mathematical Institute, a premier research institute of India where 7 was replaced by 3.

This became the basis of the following

Theorem 1.2 ([3], Saikia-Vogrinc)**.** *A natural number $p > 1$ is a prime if and only if $\binom{n}{p} - \lfloor \frac{n}{p} \rfloor$ is divisible by p for every non-negative n, where $n > p+1$ and the symbols have their usual meanings.*

2. Proof of Theorem 1.2

In [3], the above theorem is proved. The authors give three different proofs, however the third proof is incomplete. We present below a completed version of that proof.

Proof. First we assume that p is prime. Now we consider n as $n = ap + b$ where a is a non-negative integer and b an integer $0 \le b < p$. Obviously,

$$\left\lfloor \frac{n}{p} \right\rfloor = \lfloor \frac{ap+b}{p} \rfloor \equiv a \ (mod\ p). \tag{2.1}$$

Now let us calculate $\binom{n}{p}$ $(mod\ p)$.

$$\begin{aligned}
\binom{n}{p} &= \binom{ap+b}{p} \\
&= \frac{(ap+b)\cdot(ap+b-1)\cdots(ap+1)\cdot ap\cdot(ap-1)\cdots(ap+b-p+1)}{p\cdot(p-1)\cdots 2\cdot 1} \\
&= \frac{a\cdot(ap+b)\cdot(ap+b-1)\cdots(ap+1)\cdot(ap-1)\cdots(ap+b-p+1)}{(p-1)\cdot(p-2)\cdots 2\cdot 1} \\
&= \frac{aX}{(p-1)!}
\end{aligned}$$

where $X = (ap+b)\cdot(ap+b-1)\cdots(ap+1)\cdot(ap-1)\cdots(ap+b-p+1)$.

We observe that there are $(p-1)$ terms in X and each of them has one of the following forms,

(a) $ap + r_1$, or

[1]Corresponding Author: manjil@gonitsora.com

(b) $ap - r_2$
where $1 \leq r_1 \leq b$ and $1 \leq r_2 \leq (p-1-b)$.
Thus any two terms from either (a) or (b) differs by a number strictly less than p and hence not congruent modulo p. Similarly, if we take two numbers - one from (a) and the other from (b), it is easily seen that the difference between the two would be $r_1 + r_2$ which is at most $(p-1)$ (by the bounds for r_1 and r_2); thus in this case too we find that the two numbers are not congruent modulo p. Thus the terms in X forms a reduced residue system modulo p and so, we have,

$$X \equiv (p-1)! \ (mod\ p) \tag{2.2}$$

Thus using (2) we obtain,

$$\binom{n}{p} = a\frac{X}{(p-1)!} \equiv a \ (mod\ p) \tag{2.3}$$

So, (1) and (3) combined gives

$$\left\lfloor \frac{n}{p} \right\rfloor \equiv \binom{n}{p} \ (mod\ p). \tag{2.4}$$

So, forward implication is proved.

To prove the reverse implication, we adopt a contrapositive argument meaning that if p were not prime (that is composite) then we must construct an n such that (4) does not hold. So, let q be a prime factor of p. We write p as $p = q^x k$, where $(q,k) = 1$. In other words, x is the largest power of q such that $q^x | p$ but $q^{x+1} | p$ (in notation, $q^x || p$). By taking, $n = p + q = q^x k + q$, we have

$$\binom{p+q}{p} = \binom{p+q}{q} = \frac{(q^x k + q)(q^x k + q - 1)\dots(q^x k + 1)}{q!}$$

which after simplifying the fraction equals $(q^{x-1}k+1)\frac{(q^x k+q-1)\dots(q^x k+1)}{(q-1)!}$. Clearly, $(q^x k+q-1)\dots(q^x k+1) \equiv (q-1)! \not\equiv 0 \ (mod\ q^x)$. Therefore,

$$\frac{(q^x k + q - 1)\dots(q^x k + 1)}{(q-1)!} \equiv 1 \ (mod\ q^x)$$

and

$$\binom{p+q}{p} \equiv q^{x-1}k + 1 \ (mod\ q^x).$$

On the other hand obviously,

$$\left\lfloor \frac{p+q}{p} \right\rfloor = \left\lfloor \frac{q^x k + q}{q^x k} \right\rfloor \equiv 1 \ (mod\ q^x).$$

Now, since $(q,k) = 1$, it follows that $q^{x-1}k + 1 \not\equiv 1 \ (mod\ q^x)$. So we conclude,

$$\binom{p+q}{p} \not\equiv \left\lfloor \frac{p+q}{p} \right\rfloor \ (mod\ q^x). \tag{2.5}$$

So, $p \nmid (\binom{p+q}{p} - \lfloor \frac{p+q}{p} \rfloor)$, for if $p | (\binom{p+q}{p} - \lfloor \frac{p+q}{p} \rfloor)$, then since $q^x | p$, we would have $q^x | (\binom{p+q}{p} - \lfloor \frac{p+q}{p} \rfloor)$, a contradiction to (5). Thus, $\binom{p+q}{p} \not\equiv \lfloor \frac{p+q}{p} \rfloor \ (mod\ p)$. Hence we are through with the reverse implication too.

This completes the proof of Theorem 1.2. □

3. Consequences

Let $\mathrm{ord}_p(n)$ for $n \in \mathbb{N}$, be the greatest exponent of p with p a prime in the decomposition of n into prime factors,

$$\mathrm{ord}_p(n) = \max\left\{k \in \mathbb{N} : p^k | n\right\}.$$

For $x = a/b$ ($x \in \mathbb{Q}$) written in lowest terms with $\gcd(a,b) = 1$, we define $\mathrm{ord}_p(x)$ as

$$\mathrm{ord}_p(x) = \mathrm{ord}_p(a/b) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b). \tag{3.1}$$

We have the property

$$\operatorname{ord}_p(xy) = \operatorname{ord}_p(x) + \operatorname{ord}_p(y) \ \forall\, x, y \in \mathbb{Q}. \tag{3.2}$$

In view of (3.1) and (3.2), the function ord_p behaves like a logarithm. Clearly [1],

$$\operatorname{ord}_p(n!) = \sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

For $n \geq p$ such that the base p expansion of n is given by (5.1),

$$\operatorname{ord}_p(n!) = \sum_{k=1}^{s} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

In particular setting $n = p^k$ in the above,

$$\operatorname{ord}_p((p^k)!) = 1 + p + p^2 + \ldots + p^{k-1} \tag{3.3}$$

with $k \in \mathbb{N},\ k > 1$.

From the relations,

$$\begin{aligned}
\left\lfloor \frac{n}{p} \right\rfloor &= a_1 + a_2 p + \ldots + a_s p^{s-1}, \\
\left\lfloor \frac{n}{p^2} \right\rfloor &= a_2 + a_3 p + \ldots + a_s p^{s-2}, \\
&\ \vdots \\
\left\lfloor \frac{n}{p^{s-1}} \right\rfloor &= a_{s-1} + a_s p, \\
\left\lfloor \frac{n}{p^s} \right\rfloor &= a_s,
\end{aligned}$$

we get

$$\operatorname{ord}_p(n!) = a_1 + a_2 + \ldots + a_s + (a_2 + a_3 + \ldots + a_s)p + (a_3 + a_4 + \ldots + a_s)p^2 + \ldots + a_s p^{s-1}. \tag{3.4}$$

Similarly, from

$$\begin{aligned}
\left\lfloor \frac{n-p}{p} \right\rfloor &= a_1 - 1 + a_2 p + \ldots + a_s p^{s-1}, \\
\left\lfloor \frac{n-p}{p^i} \right\rfloor &= a_i + a_{i+1} p + \ldots + a_s p^{s-i}, \\
\left\lfloor \frac{n-p}{p^s} \right\rfloor &= a_s,
\end{aligned}$$

with $i = 2, 3, \ldots, s-1$, we have

$$\operatorname{ord}_p((n-p)!) = \operatorname{ord}_p(n!) - 1. \tag{3.5}$$

The above relation holds for $n > p$.

In particular when $n - p < p$, $\lfloor \frac{n-p}{p^i} \rfloor = 0$ for $i \geq 1$ and we have

$$\begin{aligned}
\operatorname{ord}_p((n-p)!) &= 0 \text{ for } n - p < p, \\
\operatorname{ord}_p(n!) &= 1 \text{ for } n - p < p.
\end{aligned}$$

If $n - p = p$, then from (3.3),

$$\begin{aligned}
\operatorname{ord}_p((n-p)!) &= 1 \text{ for } n - p = p, \\
\operatorname{ord}_p(n!) &= 2 \text{ for } n - p = p.
\end{aligned}$$

From (3.3) and (3.5) we obtain,

$$\operatorname{ord}_p\left(\binom{n}{p}\right) = \operatorname{ord}_p(n!) - \operatorname{ord}_p(p!) - \operatorname{ord}_p((n-p)!) = 1 - 1 = 0. \tag{3.6}$$

From (3.4) we have,

$$\begin{aligned}(p-1)\operatorname{ord}_p(n!) &= (a_1 + a_2 + \ldots + a_s)p - (a_1 + a_2 + \ldots + a_s)\\ &+ (a_2 + a_3 + \ldots + a_s)p^2 - (a_2 + a_3 + \ldots + a_s)p\\ &+ \ldots + (a_{s-1} + a_s)p^{s-1} - (a_{s-1} + a_s)p^{s-2}\\ &+ a_s p^s - a_s p^{s-1}.\end{aligned}$$

It gives

$$\begin{aligned}(p-1)\operatorname{ord}_p(n!) &= a_1 p + a_2 p^2 + \ldots + a_s p^s - (a_1 + a_2 + \ldots + a_s)\\ &= a_0 + a_1 p + a_2 p^2 + \ldots + a_s p^s - (a_0 + a_1 + a_2 + \ldots + a_s) \qquad .\end{aligned}$$

Setting $S_n = a_0 + a_1 + a_2 + \ldots + a_s$, we obtain

$$\operatorname{ord}_p(n!) = \frac{n - S_n}{p-1}. \tag{3.7}$$

Using (3.6) and (3.7) we deduce that,

$$S_{n-p} = S_n - 1.$$

In particular

$$\begin{aligned} n = S_n + p - 1 &\quad \text{for} \quad n - p < p,\\ S_n = 2 &\quad \text{for} \quad n - p = p,\\ S'_n = p + 1 &\quad \text{for} \quad n - p > p,\end{aligned}$$

where $S'_n = a'_0 + a'_1 + a'_2 + \ldots + a'_t$ such that,

$$n = a'_0 + a'_1(n-p) + a'_2(n-p)^2 + \ldots + a'_t(n-p)^t.$$

We know that for any prime p, $\binom{n}{p} - \lfloor \frac{n}{p} \rfloor$ is a multiple of p. Similarly, if $n-p$ is a prime, then $\binom{n}{n-p} - \lfloor \frac{n}{n-p} \rfloor$ is a multiple of $n-p$.

If $n - p < p$ with p a prime and $n \geq p$, then $\lfloor \frac{n}{p} \rfloor = \lfloor \frac{S_n - 1}{p} \rfloor + 1$ and we have $0 \leq S_n - 1 = n - p < p$. So $0 \leq \frac{S_n-1}{p} < 1$. Therefore $\lfloor \frac{S_n-1}{p} \rfloor = 0$ and hence

$$\left\lfloor \frac{n}{p} \right\rfloor = 1 \text{ for } n - p < p.$$

Thus, if p is a prime then we have $(n \geq p)$

$$\binom{n}{p} \equiv 1 \pmod{p} \text{ for } n - p < p.$$

If $n - p = p$ with p a prime, then $n = 2p$ and $S_n = 2$. Clearly,

$$\binom{2p}{p} \equiv 2 \pmod{p}.$$

If $n-p > p$ with p a prime, then $S'_n = p+1$ and so $\lfloor \frac{n}{n-p} \rfloor = \lfloor \frac{S'_n - 1}{n-p} \rfloor + 1$. Since $0 < S'_n - 1 = p < n-p$ and so $0 < \lfloor \frac{S'_n-1}{n-p} \rfloor < 1$, it follows that

$$\left\lfloor \frac{n}{n-p} \right\rfloor = 1 \text{ for } n - p > p.$$

Hence, if $n-p$ is a prime then we have,

$$\binom{n}{p} \equiv \binom{n}{n-p} \equiv 1 \pmod{n-p} \text{ for } n - p > p \text{ with } n - p \text{ prime}.$$

Remark 3.1. *A natural number $n > 3$ is equal to the sum of two primes p, q (with $q = n - p$) if either $n = 2 + p$ with $p > 2$ (in such a case, $q = 2$ and n odd) or n is even with either $p > 2$ and $q > 2$ or $p = q = 2$ (in particular, it is verified when $n = 2p$ with $p = q \geq 2$). Notice that in general, these two primes p, q are not unique. For instance, $10 = 5 + 5 = 3 + 7$. This is in essence the famous Goldbach's conjecture.*

4. Generalization of Theorem 1.2

We state and prove the following generalization of Theorem 1.2

Theorem 4.1. *For $n = ap + b = a_{(k)}p^k + b_{(k)}$, we have*

$$\binom{a_{(k)}p^k + b_{(k)}}{p^k} - \left\lfloor \frac{a_{(k)}p^k + b_{(k)}}{p^k} \right\rfloor \equiv 0 \pmod{p}$$

with p a prime, $0 \leq b_{(k)} \leq p^k - 1$ and k a positive integer such that $1 \leq k \leq l$, where

$$n = a_0 + a_1 p + \ldots + a_k p^k + a_{k+1} p^{k+1} + \ldots + a_l p^l$$

and for $k \geq 1$

$$a_{(k)} = a_k + a_{k+1} p + \ldots + a_l p^{l-k}$$

and

$$b_{(k)} = a_0 + a_1 p + \ldots + a_{k-1} p^{k-1}.$$

.

The proof of this follows from the reasoning of the proof of Theorem 1.2 although there are some subtleties.

In particular, we have

$$a = a_{(1)} = a_1 + a_2 p + \ldots + a_l p^{l-1}$$

and

$$b = b_{(0)} = a_0.$$

For $k = 0$, we set the convention that $a_{(0)} = n = a_0 + a_1 p + \ldots + a_l p^l$ and $b_{(0)} = 0$. Notice that Theorem 4.1 is obviously true for $k = 0$. But the case $k = 0$ doesn't correspond really to a power of p where p is a prime.

Proof. We have

$$\binom{n}{p^k} = \binom{a_{(k)}p^k + b_{(k)}}{p^k}$$

$$= \frac{(a_{(k)}p^k + b_{(k)}) \cdot (a_{(k)}p^k + b_{(k)} - 1) \cdots (a_{(k)}p^k + 1) \cdot a_{(k)}p^k \cdot (a_{(k)}p^k - 1) \cdots (a_{(k)}p^k + b_{(k)} - p^k + 1)}{p^k \cdot (p^k - 1) \cdots 2 \cdot 1}$$

$$= \frac{a_{(k)} \cdot (a_{(k)}p^k + b_{(k)}) \cdot (a_{(k)}p^k + b_{(k)} - 1) \cdots (a_{(k)}p^k + 1) \cdot (a_{(k)}p^k - 1) \cdots (a_{(k)}p^k + b_{(k)} - p^k + 1)}{(p^k - 1) \cdot (p^k - 2) \cdots 2 \cdot 1}.$$

Thus we obtain

$$(p^k - 1)! \binom{n}{p^k} = a_{(k)} \left(\prod_{r=1}^{b} (a_{(k)}p^k + r) \right) \left(\prod_{r=1}^{p^k - 1 - b} (a_{(k)}p^k - r) \right).$$

Or $a_{(k)}p^k + r \equiv r \pmod{p^k}$ and $a_{(k)}p^k - r \equiv -r \equiv p^k - r \pmod{p^k}$ with $0 < r < p^k$. It follows

$$\left(\prod_{r=1}^{b} (a_{(k)}p^k + r) \right) \left(\prod_{r=1}^{p^k - 1 - b} (a_{(k)}p^k - r) \right) \equiv \left(\prod_{r=1}^{b} r \right) \left(\prod_{r=1}^{p^k - 1 - b} (p^k - r) \right) \pmod{p^k}.$$

Since

$$\left(\prod_{r=1}^{b} r\right)\left(\prod_{r=1}^{p^k-1-b}(p^k-r)\right)=\left(\prod_{r=1}^{b} r\right)\left(\prod_{r=b+1}^{p^k-1} r\right)=\prod_{r=1}^{p^k-1} r=(p^k-1)!$$

we have

$$\left(\prod_{r=1}^{b}(a_{(k)}p^k+r)\right)\left(\prod_{r=1}^{p^k-1-b}(a_{(k)}p^k-r)\right)\equiv(p^k-1)! \pmod{p^k}.$$

We can now write

$$\left(\prod_{r=1}^{b}(a_{(k)}p^k+r)\right)\left(\prod_{r=1}^{p^k-1-b}(a_{(k)}p^k-r)\right)=c_{(k)}p^{k(p^k-1)}+(p^k-1)!$$

with $c_{(k)}$ the quotient of the division of the product by $p^{k(p^k-1)}$. We can notice that,

$$(p^k-1)!=q(p-1)!\,p^{1+p+\ldots+p^{k-1}-k}$$

with $\gcd(p,q)=1$ and because $\mathrm{ord}_p((p^k-1)!)=1+p+\ldots+p^{k-1}-k$. Therefore we have

$$a_{(k)}c_{(k)}p^{k(p^k-1)}+(p^k-1)!\left\{a_{(k)}-\binom{n}{p^k}\right\}=0.$$

Equivalently

$$a_{(k)}c_{(k)}p^{k(p-1)(1+p+\ldots+p^{k-1})}+q(p-1)!\,p^{1+p+\ldots+p^{k-1}-k}\left\{a_{(k)}-\binom{n}{p^k}\right\}=0$$

Dividing the above equation by $p^{1+p+\ldots+p^{k-1}-k}$ we have

$$q(p-1)!\left\{a_{(k)}-\binom{n}{p^k}\right\}+a_{(k)}c_{(k)}p^{k+(k(p-1)-1)(1+p+\ldots+p^{k-1})}=0.$$

Thus

$$q(p-1)!\left\{a_{(k)}-\binom{n}{p^k}\right\}\equiv 0 \pmod{p^k}$$

Since if $m\equiv n \pmod{p^k}$ implies $m\equiv n \pmod{p}$ (the converse is not always true), we also have

$$q(p-1)!\left\{a_{(k)}-\binom{n}{p^k}\right\}\equiv 0 \pmod{p}.$$

As $q(p-1)!$ with $\gcd(p,q)=1$ and p are relatively prime, we get

$$\binom{n}{p^k}-a_{(k)}\equiv 0 \pmod{p}.$$

We finally have

$$\binom{n}{p^k}\equiv\left\lfloor\frac{n}{p^k}\right\rfloor \pmod{p}.$$

□

5. An Alternative proof of Theorem 1.2

We present below an alternative proof of Theorem 1.2. But first we state and proof an important result in elementary number theory due to E. Lucas.

Theorem 5.1 ([2],E. Lucas (1878))**.** *Let p be a prime and m and n be two integers considered in the following way,*

$$m = a_k p^k + a_{k-1}p^{k-1} + \ldots + a_1 p + a_0,$$
$$n = b_l p^l + b_{l-1}p^{l-1} + \ldots + b_1 p + b_0,$$

where all a_i and b_j are non-negative integers less than p. Then,

$$\binom{m}{n} = \binom{a_k p^k + a_{k-1}p^{k-1} + \ldots + a_1 p + a_0}{b_l p^l + b_{l-1}p^{l-1} + \ldots + b_1 p + b_0} \equiv \prod_{i=0}^{max(k,l)} \binom{a_i}{b_i} \pmod{p}.$$

Notice that the theorem is true if $a_i \geq b_i$ for $i = 0, 1, 2, \ldots, \max(k, l)$

Theorem 5.1 has been proved in [3]. We give here an alternate proof of this result.
First of all, we state and prove a few lemmas

Lemma 5.2. *If*

$$a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \equiv b_0 + b_1 X + b_2 X^2 + \ldots + b_n X^n \pmod{p}$$

then

$$a_i \equiv b_i \pmod{p}\ \forall\, i \in [[0, n]].$$

Proof. Indeed, if $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \equiv b_0 + b_1X + b_2X^2 + \cdots + b_nX^n \pmod{p}$, then there exits a polynomial $k(X) = k_0 + k_1X + k_2X^2 + \cdots + k_nX^n$ at most of degree n such that $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = b_0 + b_1X + b_2X^2 + \cdots + b_nX^n + p(k_0 + k_1X + k_2X^2 + \cdots + k_nX^n)$. This gives $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = b_0 + pk_0 + (b_1 + pk_1)X + (b_2 + pk_2)X^2 + \cdots + (b_n + pk_n)X^n$. Hence we get $a_0 = b_0 + pk_0$, $a_1 = b_1 + pk_1$, $a_2 = b_2 + pk_2$,..., $a_n = b_n + pk_n$. Or equivalently $a_0 \equiv b_0 \pmod{p}$, $a_1 = b_1 \pmod{p}$, $a_2 = b_2 \pmod{p}$,$\cdots$, $a_n = b_n \pmod{p}$.

The reciprocal implication is trivial. □

Lemma 5.3. *If the base p expansion of a positive integer n is,*

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_l p^l$$

then we have

$$n! = q a_0!(a_1p)!(a_2p^2)! \cdots (a_lp^l)!$$

with q a natural number.

Proof. Since the factorial of a natural number is a natural number, there exists a rational number q such that

$$q = \frac{n!}{a_0!(a_1p)!(a_2p^2)! \ldots (a_lp^l)!}.$$

Let S be the set,

$$S = \{x_1, x_2, \ldots, x_l\}.$$

We consider lists of elements of S where x_0 is repeated a_0 times, x_1 is repeated a_1p times,..., x_l is repeated a_lp^l times such that, $0 \leq a_i \leq p-1$ with $i \in [[0, l]]$. In such a list, there are $l+1$ unlike groups of identical elements. For instance the selection $\left(\underbrace{x_0, x_0, \ldots, x_0}_{a_0}, \underbrace{x_1, x_1, \ldots, x_1}_{a_1p}, \ldots\ldots, \underbrace{x_l, x_l, \ldots, x_l}_{a_lp^l}\right)$ is such a list of n elements which contains $l + 1$ unlike groups of identical elements.

The number of these lists is given by $\frac{n!}{a_0!(a_1p)!(a_2p^2)!\ldots(a_lp^l)!}$. It proves that the rational number q is a natural number. And, since the factorial of a natural number is non-zero (even if this number is 0 because $0! = 1$), we deduce that q is a non-zero natural number. □

Theorem 5.4. *Let $n = ap+b = a_0+a_1p+a_2p^2+\ldots+a_lp^l$ such that $0 \leq b \leq p-1$ and $0 \leq a_i \leq p-1$ with $i \in [[0, l]]$. Then $q \equiv 1 \pmod{p}$.*

Before we prove Theorem 5.4 we shall state and prove the following non-trivial lemmas.

Lemma 5.5. *The integers q and p are relatively prime.*

Proof. If $0 < q < p$, since p is prime, q and p are relatively prime.

If $q \geq p$, let us assume that p and q are not relatively prime. It would imply that there exist an integer $x > 0$ and a non-zero natural number q' such that $q = q'p^x$ with $\gcd(q', p) = 1$. Since $n! = qa_0!(a_1p)! \dots (a_{l-1}p^{l-1})!(a_lp^l)!$ we get $n! = q'p^xa_0!(a_1p)! \dots (a_lp^l)!$. It follows that $n!$ would contain a factor $a_{l+x}p^{l+x}$ such that $q' = a_{l+x}q''$ with $a_{l+x} \in [[1, p-1]]$. But, $a_{l+x}p^{l+x} > n$.

Indeed we know that $1 + p + \dots + p^l = \frac{p^{l+1}-1}{p-1}$. So $p^{l+1} = 1 + (p-1)(1 + p + \dots + p^l)$. Then $p^{l+1} > (p-1)+(p-1)p+\dots+(p-1)p^l$. Since $0 \leq a_i \leq p-1$ with $i \in [[0, l]]$, we have $0 \leq a_ip^i \leq (p-1)p^i$ with $i \in [[0, l]]$. Therefore, $p^{l+1} > a_0 + a_1p + \dots + a_lp^l$ so $p^{l+1} > n \Rightarrow a_{l+x}p^{l+x} > n$.

Since $n!$ doesn't include terms like $a_{l+x}p^{l+x} > n$ with $a_{l+x} \in [[1, p-1]]$, we obtain a contradiction. It means that the assumption $q = q'p^x$ with $x \in \mathbb{N}^\star$ and $gcd(q', p) = 1$ is not correct. So, q is not divisible by a power of p. It results that q and p are relatively prime. $\square$

We know that $n! = (ap + b)! = qa_0!(a_1p)! \dots (a_lp^l)!$ with $a = \lfloor \frac{n}{p} \rfloor$, $0 \leq a_i \leq p-1$ with $i = 0, 1, 2, \dots, p-1$ and $b = a_0$. Let $q_{a,l,1,i}$ with $0 \leq i \leq a_1 \leq a$ be the natural number

$$q_{a,l,1,i} = \frac{(ap + b - ip)!}{a_0!((a_1 - i)p)!(a_2p^2)! \dots (a_lp^l)!}.$$

In particular, we have $q = q_{a,l,1,0}$.

Lemma 5.6. $q_{a,l,1,i+1} \equiv q_{a,l,1,i} \pmod p$.

Proof. We have $(0 \leq i < a_1)$

$$\binom{ap + b - ip}{p} = \frac{q_{a,l,1,i}}{q_{a,l,1,i+1}} \binom{(a_1 - i)p}{p}$$

Or equivalently

$$q_{a,l,1,i+1} \binom{ap + b - ip}{p} = q_{a,l,1,i} \binom{(a_1 - i)p}{p}.$$

Now

$$\binom{ap + b - ip}{p} = \binom{(a - i)p + b}{p} \equiv a - i \equiv a_1 - i \pmod p,$$

and

$$\binom{(a_1 - i)p}{p} \equiv a_1 - i \pmod p.$$

Therefore

$$q_{a,l,1,i+1}(a_1 - i) \equiv q_{a,l,1,i}(a_1 - i) \pmod p.$$

Since $a_1 - i$ with $i = 0, 1, 2, \dots, a_1 - 1$ and p are relatively prime, so $q_{a,l,1,i+1} \equiv q_{a,l,1,i} \pmod p$. $\square$

Notice that $q_{a,l,1,a_1}$ corresponds to the case where $a_1 = 0$, $(a_0+a_2p^2+\dots+a_lp^l)! = q_{a,l,1,a_1}a_0!(a_2p^2)! \dots (a_lp^l)!$.

Lemma 5.7. *For $n = ap + b = a_{(k)}p^k + b_{(k)}$ with $0 \leq b_{(k)} \leq p^k - 1$ and defining ($1 \leq k \leq l$ and $0 \leq i \leq a_k$)*

$$q_{a,l,k,i} = \frac{(a_{(k)}p^k + b_{(k)} - ip^k)!}{a_0!(a_1p)! \dots ((a_k - i)p^k)! \dots (a_lp^l)!}$$

with $a_k \geq 1$, (where it is understood that when a and l appears together as the two first labels of one $q_{\dots}$, it implies that a is given by $a = a_{(1)} = (a_1a_2 \dots a_l)_p = a_1 + a_2p + \dots + a_lp^{l-1}$) we have ($0 \leq i < a_k$)

$$\binom{a_{(k)}p^k + b_{(k)} - ip^k}{p^k} = \frac{q_{a,l,k,i}}{q_{a,l,k,i+1}} \binom{(a_k - i)p^k}{p^k}$$

Additionally, $q_{a,l,k,i} \equiv q_{a,l,k,i+1} \pmod p$.

In particular for $k = 0$, we have $(0 \leq i < a_0)$,

$$ap + b = \frac{q_{a,l,0,i}}{q_{a,l,0,i+1}}(a_0 - i)$$

with $a_0 \geq 1$.

We can prove this lemma by the following a similar reasoning as earlier and hence we omit it here.

Notice that $q = q_{a,l,k,0}$. And q_{a,l,k,a_k} corresponds to the case where $a_k = 0$. Also

$$q_{a-i,l,k,0} = q_{a,l,1,i} \equiv q_{a,l,1,i+1} \pmod p,$$

with $0 \leq i < a_1$ and $a_1 \geq 1$. So, since $q_{a,l,k,j} \equiv q_{a,l,k,j+1} \pmod p$ with $0 \leq j < a_k$, we have $q_{a-i,l,k,j} \equiv q_{a-i,l,k,0} \equiv q_{a,l,1,i} \equiv q_{a,l,1,0} \pmod p$ and $q_{a-i,l,k,0} = q_{a-i,l,l,0} \equiv q_{a-i,l,l,j} \equiv q_{a-i,l,l,a_l} \equiv q_{a-i,l-1,k,0} \pmod p$.

So $q_{a-i,l,k,0} \equiv q_{a-i,l-1,k,0} \equiv \cdots \equiv q_{a-i,l,k,0} \equiv q_{a-i,1,1,0} \equiv q_{a,1,1,i} \equiv q_{a,1,1,0} \pmod p$. Or $q_{a-i,l,k,0} = q_{a,l,1,i} \equiv q_{a,l,1,0} \equiv q_{a,l,k,0} \pmod p$.

Finally we have $q = q_{a,l,k,0} \equiv q_{a,1,1,0} \pmod p$.

Lemma 5.8. *We have also the congruence* $(a_i p^i)! \equiv a_i! p^{a_i(1+p+\ldots+p^{i-1})} \pmod p$.

Proof. We proceed by induction on i.

Indeed, we have $(a_1 p)! \equiv 1p \cdot 2p \cdots (a_1 - 1)p \cdot a_1 p \pmod p$. So $(a_1 p)! \equiv a_1! p^{a_1} \pmod p$.

It follows that $(a_2 p^2)! = ((a_2 p)p)! \equiv (a_2 p)! p^{a_2 p} \equiv a_2! p^{a_2} p^{a_2 p} \pmod p$. So $(a_2 p^2)! \equiv a_2! p^{a_2(1+p)} \pmod p$.

Let us assume that $(a_i p^i)! \equiv a_i! p^{a_i(1+p+\ldots+p^{i-1})} \pmod p$.

We have $(a_{i+1} p^{i+1})! = ((a_{i+1} p^i)p)! \equiv (a_{i+1} p^i)! p^{a_{i+1} p^i} \equiv a_{i+1}! p^{a_{i+1}(1+p+\ldots+p^{i-1})} p^{a_{i+1} p^i} \pmod p$. Thus $(a_{i+1} p^{i+1})! \equiv a_{i+1}! p^{a_{i+1}(1+p+\ldots+p^{i-1}+p^i)} \pmod p$.

Hence the result follows. □

We now prove Theorem 5.4.

Proof. If $a_i = 0$ for $i \in [[1, l]]$, then $n = a_0$ and we have $n! = q a_0!$ with $q = 1$. So, if $a_i = 0$ for $i \in [[1, l]]$, $q \equiv 1 \pmod p$.

Let consider the case where $a_i = 0$ for all $i > 1$, then $n = a_0 + a_1 p$ and we have $n! = q a_0! (a_1 p)!$. Then

$$q a_0! = \frac{n!}{(a_1 p)!} = (a_0 + a_1 p)(a_0 + a_1 p - 1) \ldots (a_1 p + 1) = \prod_{r=0}^{a_0 - 1} (a_1 p + a_0 - r).$$

Since $0 < a_0 - r \leq a_0$ for $r \in [[0, a_0 - 1]]$, we obtain

$$q a_0! \equiv \prod_{r=0}^{a_0 - 1} (a_0 - r) \equiv \prod_{r=1}^{a_0} r \equiv a_0! \pmod p.$$

Since $a_0!$ and p are relatively prime, we have $q \equiv 1 \pmod p$.

Since $q = q_{a,l,k,0} \equiv q_{a,l,1,0} \pmod p$, we conclude that $q \equiv 1 \pmod p$ whatever n is. □

We come back to the proof of Theorem 5.1.

Proof. Let m, n be two positive integers whose base p expansion with p a prime, are

$$m = a_0 + a_1 p + \ldots + a_k p^k,$$

and

$$n = b_0 + b_1 p + \ldots + b_k p^k,$$

such that $m \geq n$. We assume that $a_i \geq b_i$ with $i = 0, 1, 2, \ldots, \max(k, l)$. We denote $a = \lfloor \frac{m}{p} \rfloor$ and $b = \lfloor \frac{n}{p} \rfloor$. Since $a_i \geq b_i$ with $i = 0, 1, 2, \ldots, \max(k, l)$, we have $a \geq b$. We define

$$a_{max(k,l)} = \begin{cases} 0 & \text{if} \quad k < l \\ a_k & \text{if} \quad k \geq l \end{cases}$$

and

$$b_{max(k,l)} = \begin{cases} b_l & \text{if} \quad k \leq l \\ 0 & \text{if} \quad k > l \end{cases}$$

In particular if $\max(k,l) = k$, $b_i = 0$ for $i > l$ and if $\max(k,l) = l$, $a_i = 0$ for $i > k$.

Using these

$$m! = q_{a,k,1,0} a_0!(a_1 p)! \dots (a_k p^k)!,$$

$$n! = q_{b,l,1,0} b_0!(b_1 p)! \dots (b_l p^l)!,$$

and

$$(m-n)! = q_{a-b,k,1,0}(a_0 - b_0)!((a_1 - b_1)p)! \dots ((a_k - b_k)p^k)!.$$

We have

$$\binom{m}{n} = \frac{q_{a,k,1,0}}{q_{b,l,1,0} q_{a-b,k,1,0}} \binom{a_0}{b_0} \binom{a_1 p}{b_1 p} \dots \binom{a_{\max(k,l)} p^{\max(k,l)}}{b_{\max(k,l)} p^{\max(k,l)}}.$$

Rearranging

$$q_{b,l,1,0} q_{a-b,k,1,0} \binom{m}{n} = q_{a,k,1,0} \binom{a_0}{b_0} \binom{a_1 p}{b_1 p} \dots \binom{a_{\max(k,l)} p^{\max(k,l)}}{b_{\max(k,l)} p^{\max(k,l)}}.$$

Since $q_{a,k,1,0} \equiv q_{b,l,1,0} \equiv q_{a-b,k,1,0} \equiv 1 \pmod p$, we get

$$\binom{m}{n} \equiv \binom{a_0}{b_0} \binom{a_1 p}{b_1 p} \dots \binom{a_{\max(k,l)} p^{\max(k,l)}}{b_{\max(k,l)} p^{\max(k,l)}} \pmod p.$$

Notice that if for some i, $a_i = 0$, then $b_i = 0$ since we assume that $a_i \geq b_i$ and $b_i \geq 0$. In such a case $\binom{a_i p^i}{b_i p^i} = \binom{a_i}{b_i} = 1$.

We assume that $a_i \geq 1$. For $k \in [[1, a_i p^i - 1]]$ and for $i \in [[0, \max(k,l)]]$ with $1 \leq a_i \leq p^i - 1$, $\binom{a_i p^i}{k} \equiv 0 \pmod p$

Therefore for $a_i = 1$ we have

$$(1+x)^{p^i} = \sum_{k=0}^{p^i} \binom{p^i}{k} x^k \equiv 1 + x^{p^i} \pmod p,$$

and for any $a_i \in [[1, p^i - 1]]$

$$(1+x)^{a_i p^i} = ((1+x)^{p^i})^{a_i} \equiv (1 + x^{p^i})^{a_i} \pmod p.$$

Now comparing

$$(1+x)^{a_i p^i} = \sum_{k=0}^{a_i p^i} \binom{a_i p^i}{k} x^k,$$

and

$$(1 + x^{p^i})^{a_i} = \sum_{l=0}^{a_i} \binom{a_i}{l} x^{l p^i}$$

we get by taking $k = b_i p^i$ and $l = b_i$,

$$\binom{a_i p^i}{b_i p^i} \equiv \binom{a_i}{b_i} \pmod p.$$

Finally we have

$$\binom{m}{n} \equiv \binom{a_0}{b_0} \binom{a_1}{b_1} \dots \binom{a_{\max(k,l)}}{b_{\max(k,l)}} \pmod p.$$

$\square$

We now prove Theorem 1.2.

Proof. As above the base p expansion of a natural number $n \geq p$ with p a prime, is given by,

$$n = a_0 + a_1 p + a_2 p^2 + \ldots + a_s p^s \tag{5.1}$$

such that $0 \leq a_i \leq p-1$ with $i = 0, 1, 2, \ldots, s$ and $s \geq 1$. Clearly,

$$\left\lfloor \frac{n}{p} \right\rfloor = a_1 + a_2 p + \ldots + a_s p^{s-1}.$$

Therefore,

$$\left\lfloor \frac{n}{p} \right\rfloor \equiv a_1 \pmod{p}.$$

From Theorem 5.1, it can be observed that

$$\binom{n}{p} \equiv \binom{a_0}{0}\binom{a_1}{1}\binom{a_2}{0}\cdots\binom{a_s}{0} \pmod{p}.$$

Since $\binom{a_i}{0} = 1$ with $i \in [[0, s]] - \{1\}$ and $\binom{a_1}{1} = a_1$, we get

$$\binom{n}{p} \equiv a_1 \pmod{p}.$$

Thus,

$$\binom{n}{p} - \left\lfloor \frac{n}{p} \right\rfloor \equiv 0 \pmod{p}.$$

We deduce that if p is a prime and n a natural number which is greater than p $(n > p+1)$, then p divides $\binom{p+q}{p} - \lfloor \frac{p+q}{p} \rfloor$. ∎

Remark 5.9. *It can be noticed that*

$$n = \left\lfloor \frac{n}{p} \right\rfloor p + a_0.$$

So the proof can be done in a more concise way. Since $0 \leq a_0 \leq p-1$, we have,

$$\binom{n}{p} = \binom{\left\lfloor \frac{n}{p} \right\rfloor p + a_0}{p} \equiv \binom{a_0}{0}\binom{\left\lfloor \frac{n}{p} \right\rfloor}{1} \pmod{p}.$$

After straightforward simplifications we obtain,

$$\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \pmod{p}.$$

6. Further Results

We state here few results that can be derived mainly from Theorem 1.2. The proofs of these results can be found at [4].

Theorem 6.1. *The sequence $a_n = \binom{n}{x} \pmod{m}$ is periodic, where $x, m \in \mathbb{N}$.*

The proof of the above theorem is based on mathematical induction.

The above theorem states that for every m the sequence $a_n = \binom{n}{m} \pmod{m}$ is periodic. The next most natural question to ask is, what is the minimal length of the period? Which gives us

Theorem 6.2. *For a natural number $m = \prod_{i=1}^{k} p_i^{b_i}$, the sequence $a_n = \binom{n}{m} \pmod{m}$ has a period of minimal length,*

$$l(m) = \prod_{i=1}^{k} p_i^{\lfloor \log_{p_i} m \rfloor + b_i}$$

The idea of the proof of the above theorem is to show that the length of the period of the sequence must be a multiple of the number $\prod_{i=1}^{k} p_i^{\lfloor \log_{p_i} m \rfloor + b_i}$. Then the authors show that this must indeed be the length of the period.

The above theorem gives us very easily the following two corollaries,

Corollary 6.3. *For every positive integer $m = \prod_{i=1}^{k} p_i^{b_i}$ we have $m^2 | l(m)$.*

Corollary 6.4. *m has only one prime factor ($m = p^b$ where p is prime) if and only if $l(m) = m^2$.*

We donot prove the corollaries here, as it is quite evident that they follow from the previous theorem.

We can generalize Theorem 6.2 as follows,

Theorem 6.5. *For a natural number $m = \prod_{i=1}^{k} p_i^{b_i}$, the sequence (a_n) such that $a_n \equiv \binom{n}{x} \pmod m$ has a period of minimal length*

$$l(m,x) = \prod_{i=1}^{k} p_i^{\lfloor \log_{p_i} x \rfloor + b_i} = m \prod_{i=1}^{k} p_i^{\lfloor \log_{p_i} x \rfloor}.$$

The proof of this theorem follows from the proof of Theorem 6.2 as given in [4].

The following is an easy consequence of Theorem 6.2,

Corollary 6.6. *For $m = \prod_{i=1}^{k} p_i^{b_i}$,*

$$m^2 \leq l(m) \leq m^{k+1}.$$

Remark 6.7. *Here $k \leq m - \varphi(m)$, where φ is the Euler totient function.*

Remark 6.8. *If we define $\binom{-n}{m}$ for n a positive integer as $\binom{-n}{m} = \frac{\prod_{i=0}^{m-1}(-n-i)}{m!}$, we can observe that:*

$$\binom{-n}{m} = (-1)^m \frac{\prod_{i=0}^{m-1}(n+i)}{m!} = (-1)^m \frac{n(n+1)\dots(n+m-1)}{m!} = (-1)^m \frac{(n+m-1)!}{m!(n-1)!}.$$

So,

$$\binom{-n}{m} = (-1)^m \binom{n+m-1}{m}.$$

Since $\binom{n+l(m)}{m} \equiv \binom{n}{m} \pmod m$, it implies that

$$\binom{l(m)-n}{m} \equiv (-1)^m \binom{n+m-1}{m} (\mathrm{mod} m).$$

In particular, when $m = p$ is prime, we obtain

$$\binom{p^2-n}{p} + \binom{n+p-1}{p} \equiv 0 \pmod p.$$

The authors also state in [4] a result which is stronger than Theorem 1.2 as given below.

Theorem 6.9. *A natural number $p > 1$ is a prime if and only if $\binom{q}{p} - \lfloor \frac{q}{p} \rfloor$ is divisible by p for every prime q, where the symbols have their usual meaning.*

The proof of this result depends partly on the following famous result in number theory

Theorem 6.10 (Dirichlet (1837))**.** *If a and b are relatively prime positive integers, then the arithmetic progression $a, a+b, a+2b, a+3b, \cdots$ contains infinitely many primes.*

and also on the following two lemmas.

Lemma 6.11. *Let n be relatively prime to m. Then,*

$$\binom{n}{m} \equiv \binom{n-1}{m} \pmod m.$$

Lemma 6.12. *Let m be even. Then for every integer k we have,*

$$\binom{m+k}{m} \equiv \binom{l(m)-1-k}{m} \pmod m.$$

Indeed it is very easy to see that the result in Theorem 6.9 follows immediately for p, a prime from Theorem 1.2. To prove the other implication it is necessary to construct a counterexample for each composite p. The authors divide this construction into two parts, one when p is even and the other when p is odd. The result is derived using the lemmas mentioned above and Theorems 6.10 and Theorem 6.2.

7. Acknowledgements

The authors are grateful to Professor Nayandeep Deka Baruah for going through an earlier version of this work and offering various helpful suggestions which helped to make the presentation much clearer. The authors are also thankful to Ankush Goswami for cleaning up the exposition in the proof of Theorem 1.2. The second named author would also like to thank Bishal Deb for pointing out to him a factual error in [3] and also to Parama Dutta for a careful reading of the first two sections of this paper.

References

[1] D. M. Burton, *Elementary Number Theory*, 6 ed., Tata McGraw–Hill, 2010.

[2] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques*, Amer. J. Math., **1** (2), 184–196; **1** (3), 197–240; **1** (4), 289–321 (1878).

[3] M. P. Saikia, J. Vogrinc, *A Simple Number Theoretic Result*, J. Assam Acad. Math., **3**, Dec., 91-96, 2010 (`arXiv:1207.6707 [math.NT]`).

[4] M. P. Saikia, J. Vogrinc, *Binomial Symbols and Prime Moduli*, J. Ind. Math. Soc., **79**, (1-4), 137-143, 2011.

Lycée professionnel hotelier La Closerie, 10 rue Pierre Loti - BP 4, 22410 Saint-Quay-Portrieux, France
E-mail address: `laugier.alexandre@orange.fr`

Department of Mathematical Sciences, Tezpur University, Napaam, Sonitpur, Assam, Pin-784028, India
E-mail address: `manjil@gonitsora.com`